



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/003,820	10/31/2001	Richard Paul Tarquini	10017334-1	4709

7590 11/05/2007  
HEWLETT-PACKARD COMPANY  
Intellectual Property Administration  
P.O. Box 272400  
Fort Collins, CO 80527-2400

EXAMINER
----------

COLIN, CARL G

ART UNIT	PAPER NUMBER
----------	--------------

2136

MAIL DATE	DELIVERY MODE
-----------	---------------

11/05/2007

PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.



UNITED STATES PATENT AND TRADEMARK OFFICE

---

Commissioner for Patents  
United States Patent and Trademark Office  
P.O. Box 1450  
Alexandria, VA 22313-1450  
[www.uspto.gov](http://www.uspto.gov)

**BEFORE THE BOARD OF PATENT APPEALS  
AND INTERFERENCES**

Application Number: 10/003,820  
Filing Date: October 31, 2001  
Appellant(s): TARQUINI ET AL.

**MAILED**

**NOV 01 2007**

**Technology Center 2100**

---

Jody C. Bishop  
For Appellant

**EXAMINER'S ANSWER**

This is in response to the appeal brief filed on July 26, 2007 appealing from the Office action mailed on May 15, 2007.

**(1) Real Party in Interest**

A statement identifying by name the real party in interest is contained in the brief.

**(2) Related Appeals and Interferences**

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

**(3) Status of Claims**

The statement of the status of claims contained in the brief is correct.

**(4) Status of Amendments After Final**

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

**(5) Summary of Claimed Subject Matter**

The summary of claimed subject matter contained in the brief is correct.

**(6) Grounds of Rejection to be Reviewed on Appeal**

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

**(7) Claims Appendix**

The copy of the appealed claims contained in the Appendix to the brief is correct.

**(8) Evidence Relied Upon**

2002/0078381	FARLEY ET AL	6-2002
6,279,113	VAIDYA	8-2001

**(9) Grounds of Rejection**

The following ground(s) of rejection are applicable to the appealed claims:

**Claims 1-7** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent Publication US 2002/0078381 to **Farley et al** in view of US Patent 6,279,113 **Vaidya**.

**As per claim 1:** **Farley et al** discloses a node of a network for managing an intrusion protection system, the node (security management system (20) in fig.2) comprising: a memory module for storing data in machine-readable format for retrieval and execution by a central processing unit (see page 5, paragraph 64); and discloses the security management comprises program modules that may be implemented in conjunction with operating system programs and operable to execute an intrusion protection system management application (such as fusion engine) (see pages 3-4 paragraphs 45-47); **Farley et al** further discloses the fusion engine operable to receive text-file input (raw events or event log file) from an input device (event collector) the text file defining a network exploit rule and comprising at least one field (see page 8, paragraph 93 and page 6, paragraph 66); and comprising at least one field (see fig. 5B-5F) from which a determination is made as to whether an intrusion protection evaluates the network exploit rule (see page 7, paragraph 77 and page 14, paragraph 162); **Farley et al** discloses among others historical frequency value (see page 15, paragraphs 168-171), vulnerability status (page 13, paragraph 155), priority status values (page 14, paragraphs 160-161) for determining whether a network exploit rule has been evaluated and further discloses reason for changing the priority value is recorded so as one can determine why a particular event was assigned a reduced priority (see page 14, paragraph 167 and page 15, paragraphs 170-171). **Farley et al** is silent about the operating system comprising a network stack comprising a protocol driver and a media access control driver. These are well known features as disclosed in OSI model architecture. **Vaidya**

Art Unit: 2135

in an analogous art discloses detecting intrusion attempts into system resources by monitoring for attack signatures comprising monitoring network data to determine whether data is associated with a network intrusion; extraction of the packet information (MAC header information, IP header information, transport header information, and application information), enables the data collector to detect network intrusions based in the different layers of the OSI model (see column 7, lines 18-24). Therefore, it would have been obvious to one ordinary skill in the art at the time the invention was made to use an operating system with network stack comprising protocol driver and a media access control driver because it would allow the operating system to interpret the information collected from the packets in order to analyze and detect network intrusions as suggested by **Vaidya**.

**As per claim 2:** the references as combined above disclose the claimed node of claim 1. **Farley et al** discloses at least one field comprises vulnerability status (enabled) (page 13, paragraph 155) and priority status (severity) (paragraphs 160-161) that meets the recitation of at least one field comprises a field selected from the group consisting of an ENABLED field and a SEVERITY field.

**As per claim 3:** the references as combined above disclose the claimed node of claim 1. **Farley et al** further discloses wherein the node is operable to compile the text-file into a machine-readable signature-file and transmit the machine-readable signature-file to at least one other node of the network (see page 6, paragraphs 66-68 and page 8, paragraph 93) (generating raw event,

Art Unit: 2135

organizing, correlating them and sending them to console which is interpreted as meeting the claimed limitation of compiling and transmitting).

**As per claim 4:** the references as combined above disclose the claimed node of claim 1. **Farley et al** further discloses the node operable to store a plurality of text-files, each respectively defining a network-exploit rule, in the database (see page 8, paragraphs 97-98 and fig. 2).

**As per claim 5:** the references as combined above disclose the claimed node of claim 2. **Farley et al** further discloses a machine readable signature-file database operable to store a plurality of machine-readable signature-files each generated from one of a respective plurality of text-files (see page 8, paragraphs 96-97), the management application operable to transmit a subset of the plurality of machine-readable signature-files to another node connected to the network (see page 6, paragraphs 67-68 and page 8, paragraph 93). **Farley et al** further discloses the database may include a database raw event classification that contains categories of different raw events (par.18) to be forwarded to specific node (paragraph 192).

**As per claim 6:** the references as combined above disclose the claimed node of claim 5. **Farley et al** further discloses the database may include a database raw event classification that contains categories of different raw events (par.18) to be forwarded to specific node (paragraph 192); for example the database may also contains a list of raw events permitted to have priority status change and not priority permitted to have status change based on the vulnerability status value (vulnerable, not vulnerable, unknown (paragraph 155)) (see page 14, paragraphs 164, 166-

Art Unit: 2135

167) (see also another example of lists generated with priority status allowed or disallowed (see page 15, paragraph 168) that meets the recitation of wherein the subset comprises all machine-readable signature-files of the plurality of machine-readable signature-files each generated from a respective text-file having an asserted ENABLED field value.

**As per claim 7:** the references as combined above disclose the claimed node of claim 5. **Farley et al** further discloses wherein management application is operable to accept a SEVERITY threshold from the input device and the subset of signatures comprises all machine-readable signature-files respectively generated from a text-file having a SEVERITY field value equal to or greater than the threshold (see pages 8-9 paragraphs 98-99 and page 15, paragraph 171).

**Claims 8-20** are rejected under 35 U.S.C. 102(e) as being anticipated over US Patent Publication US 2002/0078381 to **Farley et al**.

**As per claim 8:** **Farley et al** discloses a method of distributing command and security updates in a network having an intrusion protection system, comprising: generating a text file (raw event or event log file) defining a network-exploit rule (see pages 6-7 paragraphs 76-77 and claim 9); specifying at least one field during generation of the text file such as historical frequency value, frequency value, or vulnerability status; each meets the recitation of at least one field selected from the group consisting of an enabled field value and a severity level field value during generation of the text file. As interpreted by Examiner, the vulnerability status (page 13, paragraph 155) may be either vulnerable or not or unknown that meets the recitation of enabled

Art Unit: 2135

field; the historical frequency value may be allowed or disallowed and further contains a threshold (see page 15, paragraphs 168-171), that meets the recitation of enabled field and a severity level field value; the priority status values meets the recitation of severity level field (paragraphs 160-161). **Farley et al** further discloses the raw events may be received as a file or being read in event log file (see claim 4 and page 19, paragraph 209. Although not using the same wording, it is apparent to one of ordinary skill in the art that **Farley et al** discloses the claimed limitation of claim 8. As interpreted by Examiner raw event comprises text generated during generation of the event as shown in (fig. 5B and 5C and paragraphs 77, 160-161 and 155) raw event is interpreted as being generated as a text file because **Farley et al** discloses each event is stored in an event storage area (claim 14), event is received in a file (claim 4).

**As per claim 9:** **Farley et al** discloses storing a plurality of text-files in a database, each text-file defining a network-exploit rule (see pages 8-9, paragraph 98).

**As per claim 10:** **Farley et al** discloses the database may include a database raw event classification that contains categories of different raw events (par.18) to be forwarded to specific node (paragraph 192) that meets the recitation of transmitting, by a management node of the network, a subset of the plurality of machine-readable signature-files to a node in the network .

**As per claim 11:** **Farley et al** discloses the database may include a database raw event classification that contains categories of different raw events (par.18) to be forwarded to specific node (paragraph 192); for example the database may also contains a list of raw events permitted



Art Unit: 2135

to have priority status change and not priority permitted to have status change based on the vulnerability status value (vulnerable, not vulnerable, unknown (paragraph 155)) (see page 14, paragraphs 164, 166-167) (see also another example of lists generated with priority status allowed or disallowed (see page 15, paragraph 168) that meets the recitation of wherein the subset comprises all machine-readable signature-files of the plurality of machine-readable signature-files each generated from a respective text-file having an asserted ENABLED field value.

**As per claim 12:** the references as combined above disclose the claimed node of claim 5.

**Farley et al** further discloses wherein management application is operable to accept a SEVERITY threshold from the input device and the subset of signatures comprises all machine-readable signature-files respectively generated from a text-file having a SEVERITY field value equal to or greater than the threshold (see pages 8-9 paragraphs 98-99 and page 15, paragraph 171).

**As per claim 13:** **Farley et al** discloses a computer-readable medium having stored thereon set of instructions to be executed, the set of instructions, when executed by a processor, cause the processor to perform a computer method of: (a reader) for reading input from an input device of the computer (paragraph 93); reading the raw event and creating raw event data objects that meets the recitation of compiling the input into a machine readable signature file comprising machine-readable logic representative of the network-exploit rule (see paragraph 93); also (see page 6, paragraphs 66-68 and page 8, paragraph 93) (generating raw event, organizing,

Art Unit: 2135

correlating them and sending them to console which is also interpreted as meeting the claimed limitation of compiling) and vulnerability status (enabled) (page 13, paragraph 155) and priority status (severity) (paragraph 161) that meets the recitation of a value of at least one field selected from the group consisting of an ENABLED field and a SEVERITY field. **Farley et al** discloses evaluating the machine readable signature file and determining the value of the at least one field of the machine readable signature file (see pages 8-9, paragraph 98 and page 14, paragraphs 161, 162, and 165). Another example is disclosed in paragraphs 168-171 with respect to evaluating and determining raw events based on frequency event types.

**As per claim 14: Farley et al** discloses comprising a set of instructions that, when executed by the processor, cause the processor to perform the computer method of specifying a SEVERITY threshold value (see paragraphs 160-161 and 171).

**As per claim 15: Farley et al** discloses the database may include a database raw event classification that contains categories of different raw events (par.18) to be forwarded to specific node (paragraph 192) that meets the recitation of transmitting the machine-readable signature file to another node of the network upon determining the value of the SEVERITY field is greater than the threshold (see pages 8-9 paragraphs 98-99 and page 15, paragraph 171).

**As per claim 16: Farley et al** discloses generating a text file from the input the text file specifying the network-exploit rule, and the at least one field, the machine readable signature file compiled from the text file (see page 6, paragraphs 66-68 and page 8, paragraph 93)

**As per claim 17: Farley et al** discloses the database may include a database raw event classification that contains categories of different raw events (par.18) to be forwarded to specific node (paragraph 192); for example the database may also contains a list of raw events permitted to have priority status change and not priority permitted to have status change based on the vulnerability status value (vulnerable, not vulnerable, unknown (paragraph 155)) (see page 14, paragraphs 164, 166-167) (see also another example of lists generated with priority status allowed or disallowed (see page 15, paragraph 168) that meets the recitation of wherein the subset comprises all machine-readable signature-files of the plurality of machine-readable signature-files each generated from a respective text-file having an asserted ENABLED field value (see also paragraph 192).

**As per claim 18: Farley et al** discloses wherein the intrusion protection system management application is further operable to determine, based at least in part on the at least one field, ones of a plurality of other nodes to which the network-exploit rule is to be distributed (see paragraph 192).

**As per claim 19: Farley et al** discloses vulnerability status (enabled) (page 13, paragraph 155) and priority status (severity) (paragraph 161) and further discloses whether adjusting priority value should be performed based on vulnerability status information (see paragraphs 164, 166, and 167) that meets the recitation of wherein the ENABLED field value specifies whether the network-exploit rule is enabled for evaluation by an intrusion protection system, and wherein the SEVERITY level field value specifies a severity level of the network-exploit rule.

**As per claim 20:** Farley et al discloses distributing the network-exploit rule and the at least one field to a plurality of nodes (see paragraph 45) and determining by an intrusion protection system of each of the plurality of nodes, based at least in part on the at least one field, whether to evaluate the network-exploit rule in protecting the intrusion protection system's respective node (see paragraphs 118-119 and paragraph 167).

### **(10) Response to Argument**

Regarding independent **claim 1** and **dependent claims 2-5**, Appellant's arguments with respect to claim 1 are not persuasive. The issues presented by Appellant are: a) whether Farley teaches a text-file defining a network-exploit rule and b) whether the text-file comprising at least one field that includes information from which a determination is made as to whether an intrusion protection system evaluates the network-exploit rule. Examiner asserts that Farley discloses both issues presented herein by Appellant as explained below:

a) Farley discloses a text-file defining a network-exploit rule as follows. Farley discloses event information referred to as raw event and correlation event ("a correlation event can comprise one or more raw events") (see paragraph 20). The event information is stored in database, log file, and other memory devices as text-file (see page 10, paragraphs 110-113 and fig. 8; see also page 8, paragraphs 89 and 93). Each raw event is classified and categorized according to an event type 555, and further includes other event types such as priority status, vulnerability status, historical frequency value, and zone types that are used as a basis for reasoning or a guide for conduct or action, which meet the recitation of defining a network-exploit rule (see paragraphs 98-99, paragraph 160, paragraph 175, and figs. 5B-5D with detailed explanation). As defined in

the dictionary a rule is *a guide for conduct or action; a rule is a basic generalization that is accepted as true and that can be used as a basis for reasoning or conduct. In expert systems a statement that can be used to verify premises and to enable a conclusion to be drawn.* In addition, Farley discloses a relationship between the event types and correlation rules (see paragraphs 126-146) and as an example, event type “Attack From Attacked Host” (AFAH event) as shown in figs. 5D-5F meets the recitation of defining a network-exploit rule as it contains a text-based signature description (see paragraphs 186-187).

b) Farley discloses whether the text-file comprising at least one field that includes information from which a determination is made as to whether an intrusion protection system evaluates the network-exploit rule as follows. Farley discloses the events as data structures and a data structure inherently contains field; for instance, many fields are shown inside the boxes in figures 5B, 5C, 5E, and 5F, which contain description and values (as explained in the detailed description). Farley discloses assigning priority value to raw event as well as to correlation event based on a match (see paragraph 198 and fig. 5C). The priority value contains an original value and an adjusted value and a reason for the change so that it can be determined whether an intrusion protection system has processed the correlation event (see paragraphs 162-163, 167, and 198 and fig. 5C) that meets the recitation of comprising at least one field that includes information from which a determination is made as to whether an intrusion protection system evaluates the network-exploit rule.

Appellant’s arguments with respect to claim 1 are not persuasive. Appellant mentions that it appears that a received raw event is evaluated against all rules in the database. Examiner respectfully disagrees because the exemplary embodiment AFAH is only an example of event

Art Unit: 2135

from those listed in paragraphs 126-146 that has been evaluated for both inbound attack and outbound attack because of its definition "Attack From Attacked Host". However, it is clearly stated in paragraph 187,

"This double processing of the raw event is a unique aspect of the exemplary AFAH correlation event relative to other correlation events that can be processed by the fusion engine 22. For all of the other exemplary correlation event types described earlier, the processing of steps 745 through 780 is performed once, as should be apparent to those skilled in the art based on the descriptions of the exemplary correlation event types."

In addition, even in this exemplary embodiment appellant's statement does not hold true because each raw event type is classified in specific category associated with specific rule (see paragraphs 183-184 and 192) therefore, not all the rules in the database are evaluated. As discussed in claim 1, appellant mentions paragraph 64 for support. However, paragraph 64 that appellant relies on does not mention evaluating all the rules defined in the database. Also, "at least one field" as reciting in the claim does not necessarily mean "one single field". Examiner disagrees with Appellant's statement on page 13 that raw events do not have fields as Farley discloses the events as data structures and a data structure inherently contains field; for instance, many fields are shown inside the boxes in figures 5B, 5C, 5E, and 5F, which themselves contain description and values. Examiner disagrees with Appellant's statement on page 13 that no rule is defined in the raw events as Farley discloses only some examples of correlation events/rules in paragraphs 126-146; the values and description types in the raw events define the rules and an illustrated example is "Attack From Attacked Host" (fig. 5D-5F). Examiner disagrees with Appellant's statement on page 13 that Farley only discloses parameters (e.g. source Internet protocol address, timestamp, etc.) that pertain to a detected activity rather than defining a

network rule because Farley discloses descriptive values ” (i.e. fig. 5D-5F) that describe or define attack signatures and rules. Other values as shown in fig. 5B and 5C should be considered as well as these values in the field are being matched against signature files (specific category and lists of events classified) in the database (paragraphs 182-184).

Appellant’s arguments with respect to dependent claims 2-5 are not persuasive for the same reasons discussed above with respect to independent claim 1 because of their dependency from independent claim 1.

Appellant’s arguments with respect to **claim 6** are not persuasive. Applicant generally alleges that Farley does not disclose generating machine-readable signature files from a text file and not from a text file having an asserted enabled field value. Examiner respectfully disagrees as Farley discloses the manipulation of the signals within data structures resident in storage devices can be referred to as files (paragraph 49). Farley discloses generating event information in the database based on received raw event considered as files (see paragraphs 96-97) and the raw events can be categorized based on specific fields that are enabled (see paragraphs 98-100). Farley discloses generating correlation events (paragraphs 66-67) from raw events comprising one or more raw events (paragraph 103). More specifically, the database may also contains a list of raw events permitted to have priority status change and to not have priority status change based on the vulnerability status value (vulnerable, not vulnerable, unknown (paragraph 155) (see page 14, paragraphs 164, 166-167) (see also another example of lists generated with priority status allowed or disallowed (see page 15, paragraph 168) that meets the recitation of wherein the subset comprises all machine-readable signature-files of the plurality of machine-readable

Art Unit: 2135

signature-files each generated from a respective text-file having an asserted ENABLED field value. Regarding the dependency of claim 6 with respect to claim 5, note also that Farley discloses a distributed network computer system which is not limited to the drawing as Farley discloses each of the different components can reside on a single computer (see paragraphs 68-69) and the raw events and correlation events processed or unprocessed are transmitted to other node in the network (see paragraph 117).

Appellant's arguments with respect to **claim 7** are not persuasive. Appellant generally alleges that Farley does not disclose transmitting a subset of the plurality of machine-readable signature-files to another node connected to the network wherein the management application is operable to accept a SEVERITY threshold from the input device and the subset of signatures comprises all machine-readable signature-files respectively generated from a text-file having a SEVERITY field value equal to or greater than the threshold. Examiner respectfully disagrees as Farley discloses the manipulation of the signals within data structures resident in storage devices can be referred to as files (paragraph 49). Farley discloses a fusion engine operable to accept a SEVERITY threshold from an input device (see paragraph 163). Farley discloses generating event information in the database based on received raw event considered as files (see paragraphs 96-97) and the database comprises list of machine-readable signature-files having an event type with priority (severity) threshold value (i.e. high priority/threshold –low risk) (see paragraphs 171 and 175-176). This list can therefore be retrieved and utilized for processing (see paragraph 164). Regarding the dependency of claim 7 with respect to claim 5, note also that Farley discloses a distributed network computer system which is not limited to the drawing as



Farley discloses each of the different components can reside on a single computer (see paragraphs 68-69) and the raw events and correlation events processed or unprocessed are transmitted to other node in the network (see paragraph 117).

With respect to **claim 8 and dependent claims 9-10**, Appellant's arguments with respect to claim 8 are not persuasive. Appellant argues that the raw event does not define a network exploit rule. Examiner respectfully disagrees as Farley discloses event information referred to as raw event and correlation event ("a correlation event can comprise one or more raw events") (see paragraph 20). The event information is stored in database, log file, and other memory devices as text-file (see page 10, paragraphs 110-113 and fig. 8; see also page 8, paragraphs 89 and 93). Each raw event is classified and categorized according to an event type 555, and further includes other event types such as priority status, vulnerability status, historical frequency value, and zone types that are used as a basis for reasoning or a guide for conduct or action which meet the recitation of defining a network-exploit rule (see paragraphs 98-99, paragraph 160, paragraph 175, and figs. 5B-5D with detailed explanation). As defined in the dictionary a rule is *a guide for conduct or action; a rule is a basic generalization that is accepted as true and that can be used as a basis for reasoning or conduct. In expert systems a statement that can be used to verify premises and to enable a conclusion to be drawn.* In addition, Farley discloses a relationship between the event types and correlation rules (see paragraphs 126-146) and as an example, event type "Attack From Attacked Host" (AFAH event) as shown in figs. 5D-5F meets the recitation of defining a network-exploit rule as it contains a text-based signature description (see paragraphs 186-187).

Appellant argues that the raw event merely specify parameters (e.g. source Internet protocol address, timestamp, etc.) and fails to teach specifying an Enabled field value and a

Art Unit: 2135

Severity field value. Examiner respectfully disagrees as Farley discloses the events as data structures and a data structure inherently contains field; for instance, many fields are shown inside the boxes in figures 5B, 5C, 5E, and 5F, which contain description and values. The values are assigned to the raw events and correlation events during generation of the text-file. For example, the vulnerability status (page 13, paragraph 155) may be either vulnerable, not vulnerable, or unknown is broadly and reasonably interpreted as an Enabled field. Historical frequency value, which can be compared to a threshold value in order to determine the raw event that is being evaluated is malicious or not, can be broadly and reasonably interpreted as severity level field value (see paragraphs 170-172). Assigning priority status values comprising any of the following three values 1, 2, or 3 (see paragraph 161) reads on the claim limitation of severity level field value.

Appellant's arguments with respect to dependent claims 9-10 are not persuasive for the same reasons discussed above with respect to independent claim 8 because of their dependency from independent claim 8.

Appellant's arguments with respect to **claim 11** are not persuasive. Appellant generally alleges that Farley does not disclose generating machine-readable signature files from a text file and not from a text file having an asserted enabled field value. Examiner respectfully disagrees as Farley discloses the manipulation of the signals within data structures resident in storage devices can be referred to as files (paragraph 49). Farley discloses generating event information in the database based on received raw event considered as files (see paragraphs 96-97) and the raw events can be categorized based on specific fields that are enabled (see paragraphs 98-100).

Farley discloses generating correlation events (paragraphs 66-67) from raw events comprising one or more raw events (paragraph 103). More specifically, the database may also contains a list of raw events permitted to have priority status change and to not have priority status change based on the vulnerability status value (vulnerable, not vulnerable, unknown (paragraph 155) (see page 14, paragraphs 164, 166-167) (see also another example of lists generated with priority status allowed or disallowed (see page 15, paragraph 168) that meets the recitation of wherein the subset comprises all machine-readable signature-files of the plurality of machine-readable signature-files each generated from a respective text-file having an asserted ENABLED field value. Regarding the dependency of claim 11 with respect to claim 10, note also that Farley discloses a distributed network computer system which is not limited to the drawing as Farley discloses each of the different components can reside on a single computer (see paragraphs 68-69) and the raw events and correlation events processed or unprocessed are transmitted to other node in the network (see paragraph 117).

Appellant's arguments with respect to **claim 12** are not persuasive. Appellant generally alleges that Farley does not disclose transmitting a subset of the plurality of machine-readable signature-files to a node in the network wherein the management application is operable to accept a SEVERITY threshold from the input device and the subset of signatures comprises all machine-readable signature-files respectively generated from a text-file having a SEVERITY field value equal to or greater than the threshold. Examiner respectfully disagrees as Farley discloses the manipulation of the signals within data structures resident in storage devices can be referred to as files (paragraph 49). Farley discloses a fusion engine operable to accept a

Art Unit: 2135

SEVERITY threshold from an input device (see paragraph 163). Farley discloses generating event information in the database based on received raw event considered as files (see paragraphs 96-97) and the database comprises list of machine-readable signature-files having an event type with priority (severity) threshold value (i.e. high priority/threshold –low risk) (see paragraphs 171 and 175-176). This list is retrieved and utilized for processing (see paragraph 164). Regarding the dependency of claim 12 with respect to claim 10, note also that Farley discloses a distributed network computer system which is not limited to the drawing as Farley discloses each of the different components can reside on a single computer (see paragraphs 68-69) and the raw events and correlation events processed or unprocessed are transmitted to other node in the network (see paragraph 117).

Appellant's arguments with respect to **claim 19** are not persuasive. Appellant generally alleges that Farley does not disclose an ENABLED field value specifies whether the network-exploit rule is enabled for evaluation by an intrusion protection system. Examiner respectfully disagrees as Farley discloses a vulnerability status value as an enabled field value (page 13, paragraph 155) and this vulnerability value can be used as a basis for determination of a rule (see paragraph 164). Appellant generally alleges that Farley does not disclose a SEVERITY level field value specifies a severity level of the network-exploit rule. Examiner respectfully disagrees as Farley discloses assigning priority status values comprising any of the following three values 1, 2, or 3 (see paragraph 161).

With respect to **claim 20**, Appellant's arguments with respect to claim 20 are not persuasive. Appellant argues, "Farley appears to evaluate all rules defined in a database rather than determining based at least in part on one field whether the IPS is to evaluate such rule". Examiner respectfully disagrees because the exemplary embodiment AFAH is only an example of event from those listed in paragraphs 126-146 that has been evaluated for both inbound attack and outbound attack because of its definition "Attack From Attacked Host". However, it is clearly stated in paragraph 187,

"This double processing of the raw event is a unique aspect of the exemplary AFAH correlation event relative to other correlation events that can be processed by the fusion engine 22. For all of the other exemplary correlation event types described earlier, the processing of steps 745 through 780 is performed once, as should be apparent to those skilled in the art based on the descriptions of the exemplary correlation event types."

In addition, even in this exemplary embodiment appellant's statement does not hold true because each raw event type is classified in specific category associated with specific rule (see paragraphs 183-184 and 192); therefore, not all the rules in the database are evaluated. On page 12 of the appeal brief, appellant mentions paragraph 64 for support. However, paragraph 64 that appellant relies on does not mention all received raw events are evaluated against all the rules in the database. Also, "at least one field" as reciting in the claim does not necessarily mean "one single field".

With respect to **claim 13 and dependent claims 14 and 16**, Appellant's arguments with respect to claim 13 are not persuasive. Appellant argues that the raw event do not comprise machine readable logic representative of a network-exploit rule but merely specify parameters

(e.g. source Internet protocol address, timestamp, etc.) and fails to teach a value of at least one field selected from an Enabled field value and a Severity field value. Examiner respectfully disagrees. Farley discloses event information referred to as raw event and correlation event (“a correlation event can comprise one or more raw events”) (see paragraph 20). The event information is stored in database, log file, and other memory devices as text-file (see page 10, paragraphs 110-113 and fig. 8; see also page 8, paragraphs 89 and 93). Each raw event is classified and categorized according to an event type 555, and further includes other event types such as priority status, vulnerability status, historical frequency value, and zone types that are used as a basis for reasoning or a guide for conduct or action which meet the recitation of defining a network-exploit rule (see paragraphs 98-99, paragraph 160, paragraph 175, and figs. 5B-5D with detailed explanation). As defined in the dictionary a rule is *a guide for conduct or action; a rule is a basic generalization that is accepted as true and that can be used as a basis for reasoning or conduct. In expert systems a statement that can be used to verify premises and to enable a conclusion to be drawn.* In addition, Farley discloses a relationship between the event types and correlation rules (see paragraphs 126-146) and as an example, event type “Attack From Attacked Host” (AFAH event) as shown in figs. 5D-5F meets the recitation of defining a network-exploit rule as it contains a text-based signature description (see paragraphs 186-187).

Farley discloses the events as data structures and a data structure inherently contains field; for instance, many fields are shown inside the boxes in figures 5B, 5C, 5E, and 5F, which contain description and values. For example, the vulnerability status (page 13, paragraph 155) may be either vulnerable, not vulnerable, or unknown is broadly and reasonably interpreted as an Enabled field. Historical frequency value, which can be compared to a threshold value in order to determine the raw event that is being evaluated is malicious or not, can be broadly and

reasonably interpreted as severity level field value (see paragraphs 170-172). Assigning priority status values comprising any of the following three values 1, 2, or 3 (see paragraph 161) reads on the claim limitation of severity level field value.

Appellant's arguments with respect to dependent claims 14 and 16 are not persuasive for the same reasons discussed above with respect to independent claim 13 because of their dependency from independent claim 13.

Appellant's arguments with respect to **claim 15** are not persuasive. Appellant generally alleges that Farley does not disclose transmitting upon determining the value of the severity field is greater than the threshold. Examiner respectfully disagrees as Farley discloses specifying a SEVERITY threshold (see paragraph 163). Farley discloses generating event information in the database based on received raw event considered as files (see paragraphs 96-97) and the database comprises list of machine-readable signature-files having an event type with priority (severity) threshold value (i.e. high priority/threshold –low risk) (see paragraphs 171 and 175-176). Events that are identified as being of high priority are sent to the database for storage (see paragraphs 168 and 175). Also specific list such as high priority may be retrieved and utilized for processing (see paragraphs 164 and 168). Note also that Farley discloses a distributed network computer system which is not limited to the drawing as Farley discloses each of the different components can reside on a single computer (see paragraphs 68-69) and the raw events and correlation events processed or unprocessed are transmitted to other node in the network (see paragraph 117).

Appellant's arguments with respect to **claim 17** are not persuasive. Appellant generally alleges that Farley does not disclose transmitting upon determining the ENABLED field value is logically asserted. Examiner respectfully disagrees as Farley discloses specifying the vulnerability status field (enabled field) as either vulnerable, not vulnerable, or unknown (page 13, paragraph 155). More specifically, the database may also contains a list of raw events permitted to have priority status change and to not have priority status change based on the vulnerability status value (vulnerable, not vulnerable, unknown (paragraph 155) (see page 14, paragraphs 164, 166-167) (see also another example of lists generated with priority status allowed or disallowed (see page 15, paragraph 168). Events that are identified as being enabled are sent to the database for storage (see paragraph 175). Also specific list with vulnerability status value may be retrieved and utilized for processing (see paragraph 164). Note also that Farley discloses a distributed network computer system which is not limited to the drawing as Farley discloses each of the different components can reside on a single computer (see paragraphs 68-69) and the raw events and correlation events processed or unprocessed are transmitted to other node in the network (see paragraph 117).

#### **(11) Related Proceeding(s) Appendix**

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.




Art Unit: 2135

Respectfully submitted,

/Carl Colin/  
Patent Examiner  
October 17, 2007

Conferees:

Kambiz Zand

  
KAMBIZ ZAND  
SUPERVISORY PATENT EXAMINER

Kim Vu



HEWLETT-PACKARD COMPANY  
P.O. Box 272400  
Fort Collins, Colorado 80527-24000

  
KIM VU  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100